



2134/41

PATENT
Customer No. 22,852
Attorney Docket No. 04329.2371

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
)
Motoji OOMORI et al.) Group Art Unit: 2134
)
Application No.: 09/652,157) Examiner: SIMITOSKI, Michael J.
)
Filed: August 31, 2000)
)
For: EXTENDED KEY GENERATOR,)
ENCIPHERMENT/DECIPHERMENT)
UNIT, EXTENDED KEY)
GENERATION METHOD, AND)
STORAGE MEDIUM)

RECEIVED

JUN 14 2004

Technology Center 2100

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REPLY TO OFFICE ACTION

In reply to the Office Action mailed March 8, 2004, the period for response extending to June 8, 2004, please reconsider the above-identified application in light of the following remarks.

Claims 27-46 are pending in this application. In the Office Action mailed March 8, 2004, the Examiner rejected claims 27, 28, 30, 35-37, and 39 under 35 U.S.C. § 102(b) as anticipated by Miyano (U.S. Patent No. 5,442,705); rejected claims 29, 32, 38, and 41 under 35 U.S.C. § 103(a) as unpatentable over Miyano; rejected claims 33, 42, and 46 under 35 U.S.C. § 103(a) as unpatentable over Miyano in view of Ogawa et al. (U.S. Patent No. 5,787,179); rejected claims 44 and 45 under 35 U.S.C. § 103(a) as unpatentable over Miyano in view of Srinivasan, "Random Number Generators for

Parallel Applications,” and rejected claims 34 and 43 under 35 U.S.C. § 103(a) as unpatentable over Miyano in view of Ogawa, and in further view of Schneier, “Applied Cryptography,” 2nd Edition.

The Examiner also objected to claims 31 and 40 as being dependent upon a rejected base claim but indicated they would be allowable if rewritten in independent form including all elements of each claim’s base claim and any intervening claims. Applicants thank the Examiner for the indication of allowable subject matter in this case.

Applicants respectfully traverse the rejection of claims 27, 28, 30, 35-37, and 39 under 35 U.S.C. § 102(b) as anticipated by Miyano. In order to properly anticipate Applicants’ claimed invention under 35 U.S.C. § 102(b), the Examiner must demonstrate the presence of each and every element of the claim in issue, either expressly described or under principles of inherency, in a single prior art reference. Furthermore, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claim.” See M.P.E.P. § 2121 (8th ed., Aug. 2001), *quoting* Richardson v. Suzuki Motor Co., 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Finally, “[t]he elements must be arranged as required by the claim.” M.P.E.P. § 2131 (8th ed. 2001), p. 2100-69.

Applicants’ claim 27 recites “an expansion key generation apparatus, which generates expansion keys based on input keys, the apparatus comprising a plurality of cascade-connected key transform devices, each of the key transform devices comprising,” among other things, “a nonlinear transform unit for nonlinearly transforming an output from the exclusive-OR element using a predetermined substitution table; an expansion unit for performing an expansion processing on an output from the nonlinear

transform unit; and an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key.” In making the rejection of claims 27, 35, and 36, the Examiner has not accounted for all of these features.

In particular, the cited prior art, Miyano, does not disclose or suggest all of the features of claim 27. By contrast, Miyano discloses a hardware arrangement for transforming plaintext into corresponding ciphertext using a first to n-th stages provided in tandem. Each of the first to n-th stages perform a key-dependent computation and includes a memory for storing a key, a first means for transposing, using the key, a first bit block applied from a preceding stage, second means for implementing an exclusive-or operation of output of the first means and a second bit block applied from the preceding stage, and third means for transposing out of the first means using the key. See col. 1, line 64 to col. 2, line 10.

However, these teachings do not constitute a disclosure of at least an expansion key generation apparatus, “which generates expansion keys based on input keys, the apparatus comprising a plurality of cascade-connected key transform devices, each of the key transform devices comprising,” among other things, “a nonlinear transform unit for nonlinearly transforming an output from the exclusive-OR element using a predetermined substitution table; an expansion unit for performing an expansion processing on an output from the nonlinear transform unit; and an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key,” as recited in claim 27. Accordingly, the Examiner should withdraw the rejection of claim 27.

Independent claims 35, 36, and 37, while of a different scope, include recitations similar in scope to claim 27. For at least the same reasons discussed above, the Examiner should withdraw the rejection of claims 35 and 36.

Dependent claims 28, 30, and 39 depend from allowable independent claims 27 and 37, respectively. Accordingly, the Examiner should withdraw the rejection of these dependent claims for at least the reasons discussed above.

Applicants respectfully traverse the rejection of claims 29, 32, 38, and 41 under 35 U.S.C. § 103(a) as unpatentable over Miyano. To establish a proper *prima facie* case of obviousness under 35 U.S.C. § 103(a), the Examiner must demonstrate each of three requirements. First, the reference or references, taken alone or combined, must teach or suggest each and every element recited in the claims. See M.P.E.P. § 2143.03 (8th ed. 2001). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references in a manner resulting in the claimed invention. See M.P.E.P. § 2143.01 (8th ed. 2001). Third, a reasonable expectation of success must exist. See M.P.E.P. § 2143.02 (8th ed. 2001). Moreover, each of these requirements must be found in the prior art, not in applicant's disclosure. See M.P.E.P. § 2143 (8th ed. 2001).

Claims 29, 32, 38, and 41 depend from allowable independent claims 27, 36, and 37, respectively. Accordingly, at least due to their dependencies from allowable claims, and because these dependent claims include additional elements that are neither disclosed nor suggested by Miyano, the Examiner should withdraw the rejection of claims 29, 32, 38, and 41.

In addition, regarding the Examiner's conclusion of the existence of a motivation ("as was known to do so") to modify the teachings of Miyano in the lower paragraph on page 3 and the paragraph at the top of page 4, Applicants traverse the Examiner's presumed taking of Official Notice.

Applicants refer the Examiner to the February 21, 2002 Memorandum from USPTO Deputy Commissioner for Patent Examination Policy, Stephen G. Kunin, regarding "Procedures for Relying on Facts Which are Not of Record as Common Knowledge or for Taking Official Notice." In relevant part, the Memorandum states, "If the examiner is relying on personal knowledge to support the finding of what is known in the art, the examiner must provide an affidavit or declaration setting forth specific factual statements and explanation to support the finding" (Memorandum, p. 3). Applicants submit that the Examiner has made a generalized statement regarding Applicants' claims 29, 32, 38, and 41 without any documentary evidence to support it. Applicants traverse the Examiner's presumed taking of "Official Notice," noting the impropriety of this action, as the Federal Circuit has "criticized the USPTO's reliance on 'basic knowledge' or 'common sense' to support an obviousness rejection, where there was no evidentiary support in the record for such a finding." *Id.* at 1. Applicants submit that "[d]eficiencies of the cited references cannot be remedied by ... general conclusions about what is 'basic knowledge' or 'common sense.'" In re Lee, 61 USPQ2d 1430, 1432-1433 (Fed. Cir. 2002), quoting In re Zurko, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001).

Should the Examiner maintain the rejection after considering the arguments presented herein, Applicants submit that the Examiner must provide "the explicit basis

on which the examiner regards the matter as subject to official notice and allow Applicants to challenge the assertion in the next reply after the Office action in which the common knowledge statement was made” (*Id.* at 3, emphasis in original), or else withdraw the rejection.

Applicants respectfully traverse the rejection of claims 33, 42, and 46 under 35 U.S.C. § 103(a) as unpatentable over Miyano in view of Ogawa.

Independent claim 46 recites an expansion key generation apparatus comprising, among other things, “a plurality of cascade-connected key transform devices for generating expansion keys based on input keys, each of the key transform devices comprising: a first key transform unit for nonlinearly transforming a first key obtained from the input key using a predetermined substitution table” and “an expansion key calculation unit for calculating the expansion key based on an output from the first key transform unit and a second key obtained from the input key.” As discussed above, Miyano does not disclose or suggest at least these features. In addition, Ogawa does not make up for the deficiencies of Miyano.

By contrast, Ogawa discloses a scrambling method involving supplying predetermined data included in a first stream part and having a non-fixed value to a random number generator of a de-scrambling apparatus as an initial value. See col. 2, lines 54-59. Accordingly, neither Miyano nor Ogawa, taken alone or in combination, disclose or suggest all of the features of Applicants’ claim 46.

Claims 33 and 42 depend from allowable independent claims 27 and 36, respectively. These dependent claims are thus allowable at least due to their dependencies from allowable claims.

Applicants respectfully traverse the rejection of claims 44-45 under 35 U.S.C. § 103(a) as unpatentable over Miyano in view of Srinivasan.

Independent claim 44 recites “an expansion key generation apparatus comprising, a plurality of cascade-connected key transform devices for receiving different keys and generating expansion keys based on the received keys, each of the key transform devices comprising a plurality of parallel devices, each of the parallel devices comprising,” among other things, “a register for storing a constant determined for each of the parallel devices; an expansion unit for performing an expansion processing on an output from the substitution unit; and an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key.” Miyano and Srinivasan, taken alone or in combination, do not disclose or suggest at least these features.

As discussed above, Miyano does not disclose or suggest at least these features. Nor does Srinivasan, which discloses random number generators and methods that have been used as generators on parallel computers, make up for the deficiencies of Miyano discussed above. Independent claim 45, while of a different scope, includes recitations similar to those of claim 44. Accordingly, Applicants respectfully request the Examiner to withdraw the rejection of claims 44 and 45.

Applicants respectfully traverse the rejection of claims 34 and 43 under 35 U.S.C. § 103(a) as unpatentable over Miyano in view of Ogawa, and in further view of Schneier.

Dependent claims 34 and 43 depend from allowable independent claims 27 and 36. As discussed above, Miyano and Ogawa do not disclose or suggest all of the

elements of Applicants' claims 27 and 36. Schneier, which discloses an algorithm used for encryption and decryption, does not make up for the deficiencies discussed above. Dependent claims 34 and 43 depend from allowable independent claims 27 and 36 and are thus allowable at least due to their respective dependencies from allowable claims.

Finally, Applicants respectfully traverse the objection to claims 31 and 40 as being dependent upon a rejected base claim (which the Examiner deemed allowable if rewritten in independent form including all elements of each claim's base claim and any intervening claims). Claims 31 and 40 depend from allowable independent claims 27 and 37 and are thus allowable for at least the reasons discussed above.

CONCLUSION

In view of the foregoing remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 8, 2004

By: Anthony G. L. Reg. No. 53,232
for Richard V. Burgujian
Reg. No. 31,744